УДК 658.56:65.01

ОЦЕНКА ДОСТОВЕРНОСТИ ОБНАРУЖЕНИЯ НЕГАТИВНЫХ СОБЫТИЙ КАК ДИНАМИЧЕСКАЯ ПРОЦЕДУРА В МНОГОФУНКЦИОНАЛЬНОЙ ТЕХНОЛОГИЧЕСКОЙ ПЛАТФОРМЕ «ПРОГРАММНЫЙ КОМПЛЕКС ELECTRONIKA SECURITY MANAGER»

Л.Н. ЕЛИСОВ, Н.И. ОВЧЕНКОВ

В работе рассматривается одна из функциональных процедур, реализованных в многофункциональной технологической платформе «Программный комплекс Electronika security manager». Программный комплекс представляет собой автоматизированную систему обеспечения авиационной безопасности аэропорта. Процедура выполняет динамическую оценку достоверности обнаружения негативного события.

Ключевые слова: авиационная безопасность, автоматизированная система, программный комплекс, функциональная процедура, оценка, достоверность, негативное событие.

Многофункциональная технологическая платформа «Программный комплекс Electronika Security Manager» (ESM) разработан в ООО ПСЦ «Электроника» и предназначен для решения совокупности задач по обеспечению авиационной безопасности аэропортов в соответствии с современными требованиями отечественных нормативных документов.

В рамках единой платформы решаются задачи по интеграции и управлению подсистемами безопасности аэропорта: конфигурирование оборудования; управление базами данных; сбор, обработка и анализ информации; обеспечение пользовательских интерфейсов; защита информации и разделение доступа к ней; управление подсистемами безопасности; интеграция с информационными системами управления и многие другие.

В основной набор подсистем комплекса входят: системы контроля и управления доступом, системы видеонаблюдения и видеоанализа, системы тепловизионного контроля территорий и периметров, радиолокационно-оптический комплекс, системы инженерно-технической защиты периметра, системы охранно-пожарной сигнализации, системы охранно-тревожной сигнализации, системы удаленного мониторинга объектов, системы позиционирования и мониторинга подвижных объектов, системы управления инженерными системами и коммуникациями [1; 2; 3].

Программный комплекс ESM предоставляет следующие функции (рис. 1): организацию системы контроля и управления доступом (СКУД), системы видеонаблюдения (СВН), системы охранно-тревожной и охранно-пожарной сигнализации (ОТС и ОПС), систем охранного видеонаблюдения и технологического наблюдения, а также мониторинг событий и тревог систем диспетчеризации; организацию системы сбора и обработки информации (ССОИ); верификацию проходов и тревог, получаемую на стыке систем с видеонаблюдением при интеграции; поддержку биометрической верификации; учет рабочего времени; учет персонала на объекте с контролем количества персонала на территориях в реальном времени; отображение планов объектов с техническими средствами охраны и возможностью управления техническими средствами охраны (ТСО); электронное бюро пропусков, со сканированием паспортов, вводом фотографий через видеокамеру, редактор шаблонов пропусков; WEB систему подачи заявок; систему ведения черных списков нарушителей режима с возможностью автоматического блокирования выдачи пропуска; механизм выявления инцидентов безопасности по любым событиям, фиксируемым в системе; систему управления оперативными процедурами, позволяющую автоматизировать управление разрешением инцидентов; подсистему отчетов по любым функциям ESM.

Рис. 1. Функциональная структура ESM

На рис. 2 представлены системы и оборудование, поддерживаемые в ESM.

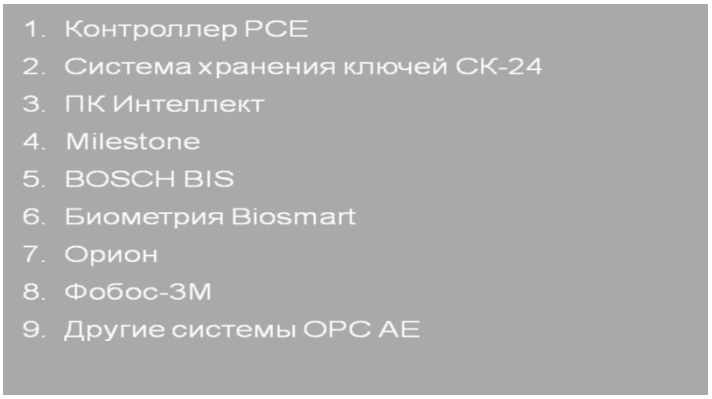

Рис. 2. Подсистемы, поддерживаемые в ESM

ESM относится к классу программных продуктов, обеспечивающих решение задачи программной интеграции различных подсистем безопасности в единый информационный комплекс. Программные системы такого класса состоят из трех крупных функциональных уровней. Уровень подключения оборудования, который решает задачи получения событий, управления интегрируемым оборудованием, унификации во внутреннее представление и управление конфигурированием. Выше находится логический уровень, который предназначен для хранения данных и алгоритмов обработки, включающий встроенные процедуры обработки данных, с возможностью настроек, а также средства для создания пользовательских алгоритмов (скрипты). Следующий уровень пользовательского интерфейса решает задачи унификации представления информации и обеспечивает единое информационное пространство для пользователей системы.

Платформа реализует следующие цели: интеграция на разных уровнях оборудования, чем обеспечивается коллекционирование данных разных систем и устройств; построение распределенных систем безопасности для организации распределенной обработки данных на локальных участках и объединения потока данных в едином центре; организация централизованного бюро пропусков на все подсистемы СКУД; построение иерархических систем мониторинга, что позволяет организовать систему мониторинга корпоративного масштаба с несколькими уровнями иерархии; применение открытой СУБД для упрощения взаимодействия с системами предприятия; обеспечение безопасности и достоверности передаваемый данных; аудит доступа к данных, который обеспечивается ведением журнала работы операторов; открытый интерфейс со сторонними системами, предоставляющий возможность реализации интеграции на любых распространенных языках программирования; интеграция видеоданных в один интерфейс и совмещение с данными из других систем, что открывает новый функционал и возможности для опера-

тора; модифицируемость, обеспечивающая настройку интерфейса и гибких алгоритмов обработки информации; производительность; надежность.

Открытость системы выражается: в поддержке оборудования и систем СОПС, СКУД, СВН различных производителей; в поддержке и широком использовании стандартных и универсальных протоколов интеграции систем различных производителей; в наличии DDK (driver development kit), предназначенном для интеграции в ESM оборудования и систем безопасности без привлечения разработчика; в наличии SDK (software development kit), предназначенном для интеграции ESM с ERP (АСУ) предприятия для обеспечения двусторонней связи с кадровой и другими службами.

Одной из важных задач, решаемых в ESM, является задача оценки достоверности обнаружения негативного события в динамике изменения параметров внешней среды [4; 5].

Сигналы от систем безопасности не являются однозначными. Тревога на периметре может быть связана с действиями нарушителя, с плохими погодными условиями, с забывчивостью сотрудника, вошедшего в не снятое с охраны помещение и т.д., т.е. сигналы от технических средств защиты аэропорта без дополнительной обработки не являются достаточными и достоверными.

Инцидент безопасности – события или набор событий, сигнализирующих о наличии угрозы или наличии негативной ситуации в охраняемом объекте.

Достоверность информации об инциденте безопасности – вероятность того, что события или набор событий сигнализируют о реальной угрозе или наличии негативной ситуации. Достоверность оценивается в процентах в диапазоне от 0% (ложная информация) до 100% (верная информация).

Достоверность информации об инциденте формируется из достоверностей событий, входящих в инцидент и основана на достоверности события, полученного от технического средства, передавшего сообщение о данном событии. При возникновении события сервер оборудования добавляет в событие атрибут "Достоверность", значение которого равно значению «вероятности ложных тревог» соответствующего объекта мониторинга. Далее модуль инцидентов в системе создает новый экземпляр инцидента и присваивает значение достоверности события (Рс) значению достоверности информации об инциденте (Ри)

$$Ри = Рс. \quad (1)$$

Если возникает новое событие, связанное с этим инцидентом, то расчет новой достоверности производится по формуле (для независимых событий)

$$Рн = 1- (1-Рт)*(1-Рс), \quad (2)$$

где Рн – новое значение достоверности инцидента; Рт – текущая достоверность инцидента; Рс – достоверность нового события.

Если хотя бы одно из событий, связанных с инцидентом, окажется достоверным, т.е. Рс = 1, то и Рн = 1. Это означает, что события инцидента связаны логической операцией «или».

Начальная вероятность ложных тревог для соответствующего объекта мониторинга задается равной 1, а в процессе работы формируется статистически. Во время эксплуатации снижаются характеристики технического средства и необходимо, чтобы система корректировала данный показатель при ложных тревогах. Для реализации данного требования необходимо:

1. Добавить к объекту мониторинга атрибуты "число ошибок" и "число событий". Атрибут «число ошибок» представляет собой счетчик ложных событий, формируемых датчиком, ассоциированным с объектом мониторинга.

2. Предоставить возможность указывать в типах объектов мониторинга события, которые формируют показатель "число событий". При обработке события система должна увеличивать значение счетчика объекта мониторинга.

3. Предоставить возможность оператору указать событие как ложное. При обработке данной команды система должна увеличить показания счетчика "число ошибок" объекта события.

4. При изменении атрибутов "число событий" и "число ошибок", система должна автоматически корректировать атрибут "вероятность ложной тревоги" по формуле

$$Вн = (Во*100+Чс-Чо) / (100+Чс), \quad (3)$$

где Во – вероятность ложной тревоги текущая; Вн – новая вероятность после фиксации ложной тревоги; Чо – число ошибок; Чс – число событий.

На рис. 3 представлен пример статистической коррекции вероятности обнаружения негативного события, построенный на 250 реальных случаях их появления.

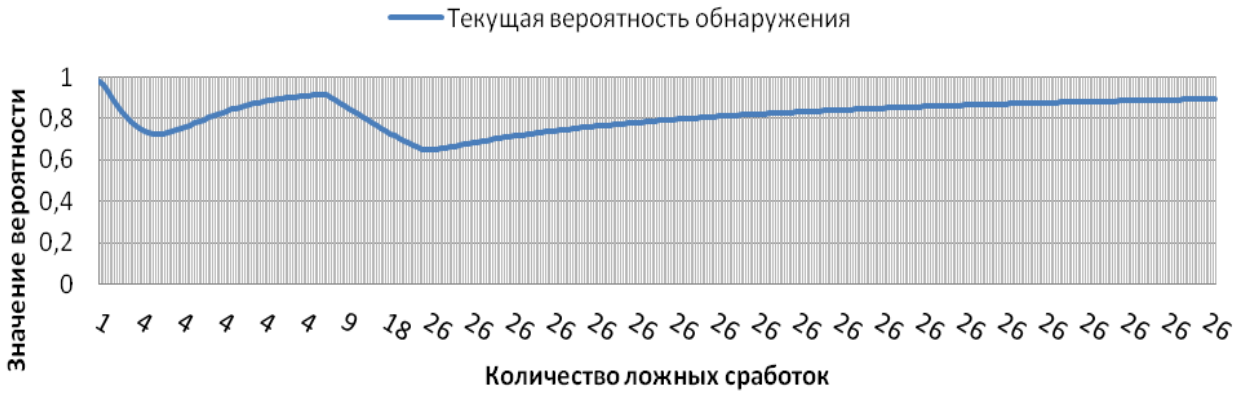

Рис. 3. Статистическая коррекция вероятности обнаружения

Программный комплекс ESM допускает существование некоторой погрешности, т.е. существует вероятность ошибки системы, которую способен различить только оператор. В таком случае система должна предоставить возможность оператору определить ложность (недостоверность) инцидента. Для этого в интерфейсе пользователя системы существует специализированная команда управления инцидентом "Пометить как ложный". В результате выполнения команды система понижает достоверность инцидента с учетом субъективных признаков, определяемых характеристиками оператора, т.е. при выполнении команды "Пометить как ложный" система использует данный показатель для формирования новой достоверности инцидента

$$Рн=Рт*Еп, \quad (4)$$

где Рн – новая достоверность события; Рт – текущая достоверность события; Еп – вероятность ошибки оператора.

Рассмотренная процедура является одной из множества функциональных операций, необходимых для решения задачи динамического управления структурой технических средств обеспечения авиационной безопасности аэропорта.

ЛИТЕРАТУРА

1. **Елисов Л.Н.** *Качество профессиональной подготовки авиационного персонала и безопасность воздушного транспорта:* монография. М.: ИЦППС, 2006. 244 с.

2. **Елисов Л.Н., Баранов В.В**. *Управление и сертификация в авиационной транспортной системе:* монография. М.: Воздушный транспорт, 1999. 352 с.

3. **Елисеев Б.П., Елисов Л.Н.** *Системотехническое управление образовательными комплексами*: монография. М.: МГТУ ГА, 2012. 208 с.

4. **Елисов Л.Н.** К вопросу о точности эвристических алгоритмов при решении оптимизационных задач в эксплуатации // *Научный Вестник МГТУ ГА*. 2012. № 179. С. 123-127.

5. **Николайкин Н.И.** *Управление экологической безопасностью промышленно-транспортных и энергетических узлов*: монография. М.: МГУИЭ, 2007. 256 с.

EVALUATION OF THE RELIABILITY OF DETECTION OF ADVERSE EVENTS AS A DYNAMIC PROCESS IN THE MULTY-TECNOLOGY PLATFORM «SOFTWARE PACKAGE ELECTRONICS MANAGERY SECURITY GUYRD»

Elisov L.N., Ovchenkov N.I.

The paper conciders one of the operational procedures implemented in the multy-functional technological. This package provides an automated system for providing airport aviation security. The procedure performs dynamic evaluation of reliability of negative events detection.

Keywords: aviation security, automated system, software system, operational procedures, evaluation, reliability, negative events.

REFERENCES

1. Elisov L.N. *Kachestvo professional'noj podgotovki aviacionnogo personala i bezopasnost' vozdushnogo transporta:* monografija. M.: ICPPS. 2006. 244 p.

2. Elisov L.N., Baranov V.V. *Upravlenie i sertifikacija v aviacionnoj transportnoj sisteme:* monografija. M.: Vozdushnyj transport. 1999. 352 p.

3. Eliseev B.P., Elisov L.N. *Sistemotehnicheskoe upravlenie obrazovatel'nymi kompleksami*: monografija. M.: MGTU GA. 2012. 208 p.

4. Elisov L.N. K voprosu o tochnosti jevristicheskih algoritmov pri reshenii optimizacionnyh zadach v jekspluatacii. *Nauchnyj Vestnik MGTU GA*. 2012. № 179. Pp. 123-127.

5. Nikolajkin N.I. *Upravlenie jekologicheskoj bezopasnost'ju promyshlenno-transportnyh i jenergeticheskih uzlov:* monografija. M.: MGUIJe. 2007. 256 p.

Сведения об авторах

Елисов Лев Николаевич, 1945 г.р., окончил ППИ (1967), профессор, доктор технических наук, действительный член Петровской академии наук и искусств, профессор кафедры безопасности полетов и жизнедеятельности МГТУ ГА, автор около 200 научных работ, область научных интересов – системотехника, квалиметрия, проблемы безопасности воздушного транспорта, авиационный персонал, авиационная безопасность.

Овченков Николай Иванович, 1966 г.р., окончил ЯрГУ им. Демидова (1990), кандидат технических наук, генеральный директор – главный конструктор ООО ПСЦ «Электроника», автор около 20 научных работ, область научных интересов – системотехника, квалиметрия, авиационная безопасность.